Distributed Industrial Control Systems Security

Decentralized Security Design in Industrial Control Systems

By: Adam Spanier, Kendra Herrmann, Matthew Popelka, Perry Donahue and Brevin Wagner

University of Nebraska Omaha

Background

Industrial Control Systems (ICS)

- Cyber-physical systems controlling industrial processes through sensing and actuating
- Use Programmable Logic Controllers (PLCs) for cyber-physical interactions
- Operate in hard-real-time environments where tasks must complete within specific timeframes
- Centralized through SCADA (Supervisory Control and Data Acquisition) systems

Decentralized Security Approaches

- **Blockchain**: Immutable time-scale transaction histories that prevent data alteration
- **Digital Signatures**: Link cryptographic keys to documents for verification and non-repudiation
- **Digital Fingerprinting**: Generates unique identifiers from device physical attributes
- **Anomalous Behavior Detection**: Identifies suspicious activity through pattern recognition

Research Questions

RQ1:

How can Distributed Industrial Control Systems be designed for security using distributed cryptographic security controls?

RQ2:

What effect, if any, do these combined mechanisms have on the security stance of ICS systems?

Research Objectives

Decentralized Cryptographic Security for Industrial Control Systems

1. Provide holistic, system-level DSC design guidance for ICS network engineers
2. Observe how different applications and combinations of DSC measures affect ICS networks
3. Understand the benefits and drawbacks of applying system-level DSC design to ICS networks

Moving beyond single-control testing to holistic security architecture

System Emulation

Unencrypted Environment

- Baseline reference for benchmarking
- No encryption or security controls
- Components: OpenPLC, MQTT Broker, InfluxDB, Grafana, SCADA
- Basic password protection only

Encrypted Environment

- Standard security mechanisms
- TLS encryption and secure protocols
- Components: OpenPLC with Modbus-TLS, MQTT (TLS-enabled), OPC-UA Server
- VPN Gateway (WireGuard) for tunneling

Blockchain Enabled Environment

- Novel decentralized security controls
- Blockchain Integrity Server for data validation
- Fingerprinting Server for anomaly detection
- Enhanced security through data integrity verification

Security Testing Approach

- All three environments undergo identical security testing via Docker containers with multi-threaded scripts that assess connectivity, authentication, encryption quality, and component-specific vulnerabilities. Results demonstrate progressive security improvements from the baseline to the DSC implementation.

System Testing

Unencrypted Environment

- Default credentials (e.g., "admin") used for PLC1 login
- Open and unsecured ports on PLC1 and Grafana
- Some components inaccessible due to configuration errors
- Minimal security relying only on basic password protection
- No encryption applied to communications

Security Model: Individual device protection

Encrypted Environment

- TLS configurations implemented
- Tighter port access controls
- Encrypted ports for components (MQTT: 8883)
- Network segmentation confirmed
- Missing security headers in Grafana

Key Issues:

- **14 critical failures**
- **Missing/improperly configured TLS support**

Security Model: Network security

Blockchain Enabled Environment

- Data integrity and fingerprinting
- Device identity verification
- Higher pass rate in security tests
- More consistent enforcement of port security

Key Improvements:

- **Enhanced data integrity verification**
- **Better detection of device impersonation**
- **Improved authentication mechanisms**

Security Model: System-wide trust

Demo

Credit: zhaojiankang

Demo

Insert Demo Video Here

Results Overview

Experimental Results

- DSC mechanisms provide more robust security stance than traditional security alone
- Fingerprinting enables anomaly detection through baseline pattern comparison
- Experimental network demonstrated superior security control design
- Detection of operations outside normal parameters indicating potential compromises

Key Findings

- Decentralized security controls in ICS are underdeveloped
- Current research focuses on single security control test environments
- Blockchains and fingerprinting are the most common DSC mechanisms

Conclusions

- DSC mechanisms used in conjunction with standard security controls provide elevated security posturing for critical systems.
- This research adds fidelity to understanding holistic design activities for ICS security.